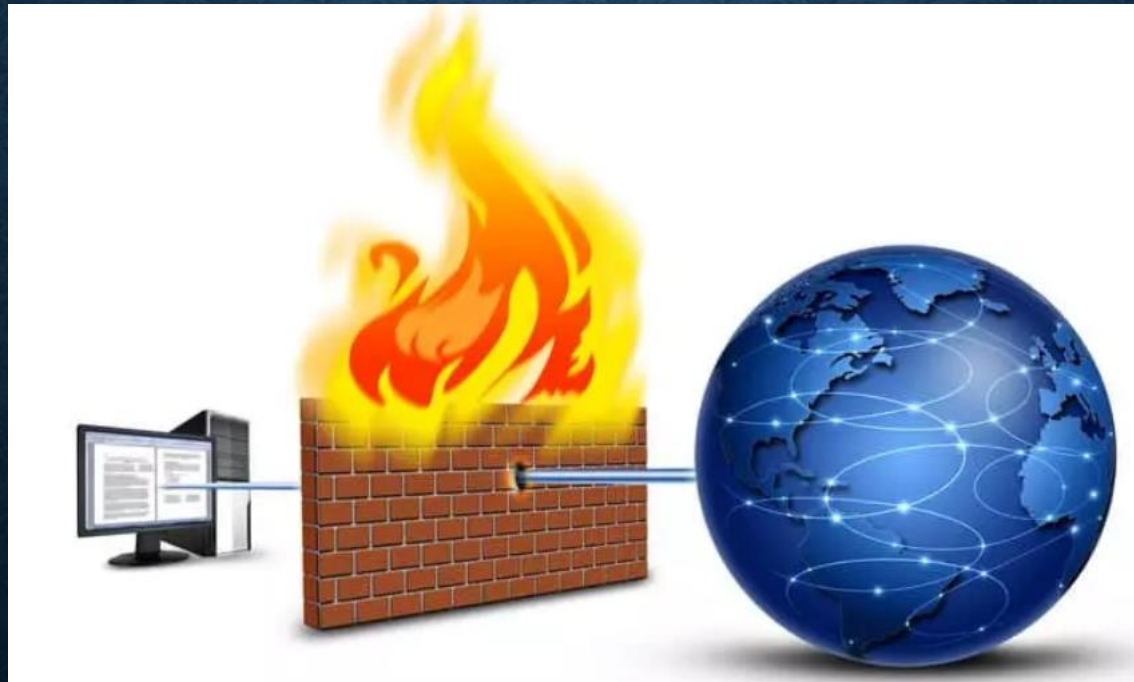


PARE-FEU (FIREWALL)



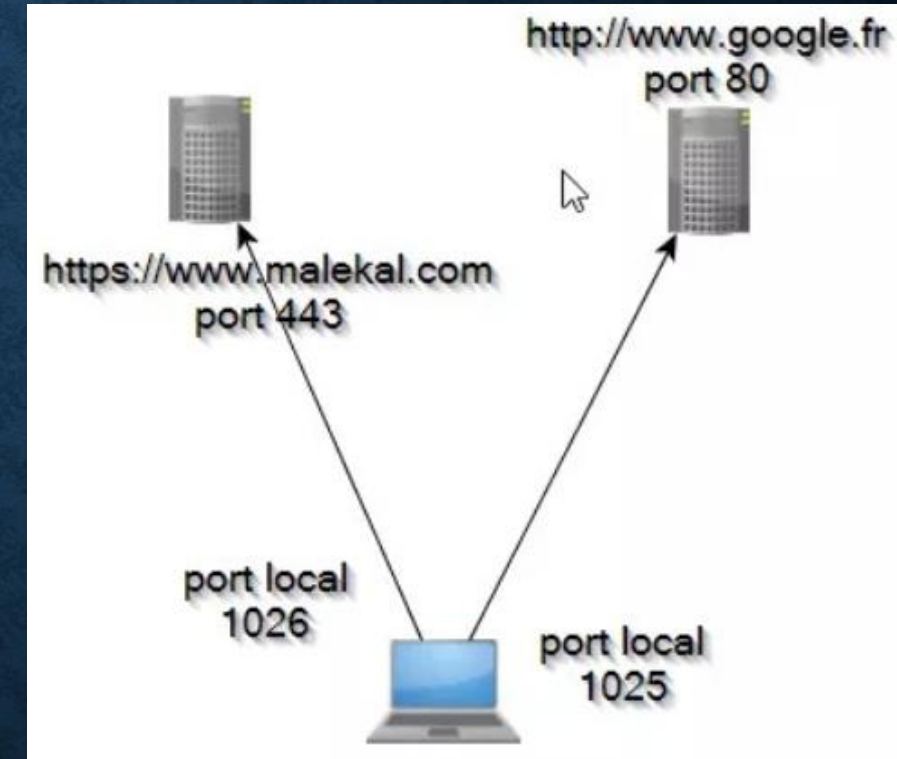
1- LES PORTS RÉSEAUX

- Lorsque l'on intéresse à la sécurité informatique, on peut entendre parler de **port réseau ouvert**.
- En effet, cela peut être utilisé comme porte d'entrée afin de s'introduire dans votre système et de pirater votre ordinateur.



LES PORTS RÉSEAUX

- Un port réseau est **un point d'entrée ou de sortie réseau** qu'une application ou le système d'exploitation peut utiliser.
- Ce dernier se caractérise par un numéro, par exemple, un serveur WEB tourne sur le port 80 (HTTP) ou 443 (HTTPS), un serveur FTP le port 21.
- Lorsque vous établissez une connexion vers une machine distante, vous vous connectez **à un port distant** en particulier.



LES PORTS RÉSEAUX – LISTE DES PORTS

- Il existe **65535** numéro de ports.
- Vous pouvez les consulter en utilisant ce line:

<https://www.crashdebug.fr/liste-des-ports-logiciels-tcp-et-udp>

PORT	SERVICE	DESCRIPTION
20	FTP Data	Port used by the FTP protocol to send data to a client
22	SSH	Used as secure replacment protocol for Telnet
23	Telnet	Port used by Telnet to remotely connect to a workstation or server
25	SMTP	Port used to send e-mail over the internet
53	DNS	Port used for DNS requests and zone transfers
80	HTTP	Protocol used for showing web pages on a browser
110	POP3	Post Office Protocol (POP3) is used to receive/read e-mail
143	IMAP	Internet Message Access Protocol (IMAP) is a new protocol to read e-mail
443	HTTPS	Port used for securing web traffic
3389	RDP	Port used by Remote Desktop to remotely manage a windows system

LES PORTS RÉSEAUX - ÉTATS DES PORTS

- Un **port ouvert** est donc un port **en écoute** et attend de connexion entrante.
- Par défaut Windows ou Mac ouvre des ports liés à des services réseaux. (Exemple: Chrome, Teams, Skype, ...) . Il est donc normal d'avoir des ports ouverts.
- Les ports réseaux ont plusieurs états:
 - **Port Ouvert :** Une application a ouvert le port et ce dernier est en écoute. Un client peut alors se connecter à ce port. Comme les serveurs Web qui écoute sur le port ouvert 80.
 - **Port Fermé:** Le port est fermé et n'accepte aucune connexion entrante.
 - **Port Filtré:** Une application réseau, comme un pare-feu (firewall), filtre l'accès sur le port. Ainsi, vous n'êtes pas capable de déterminer si le port est ouvert ou fermé.

LES PORTS RÉSEAUX - ÉTATS DES PORTS

Voici la procédure pour [lister les ports ouverts](#) sur Windows:

- Ouvrez le **Gestionnaire de tâches** puis onglet **Performances**.
- Cliquez en bas à gauche sur **Moniteur de ressources**.
- Ensuite cliquez sur l'onglet **Réseau**.
- En bas, vous avez **Connexion TCP**. Vous obtenez la liste des ports ouverts et en écoute.

Connexions TCP					
Processus	PID	Adresse locale	Port local	Adresse distante	Port distant
chrome.exe	3000	192.168.2.101	55531	172.217.13.162	443
chrome.exe	3000	192.168.2.101	55167	172.217.13.164	443
chrome.exe	3000	192.168.2.101	55152	172.217.13.110	443
chrome.exe	3000	192.168.2.101	55035	172.217.13.162	443
chrome.exe	3000	192.168.2.101	54149	104.17.8.65	443
chrome.exe	3000	192.168.2.101	53996	104.17.7.65	443
vpnagent.exe	4432	Bouclage IPv4	62522	Bouclage IPv4	49780
svchost.exe (netsvc -p)	5884	192.168.2.101	53649	52.177.165.30	443
OpenVPNConnect.exe	7536	Bouclage IPv4	60790	Bouclage IPv4	60789
OpenVPNConnect.exe	7536	Bouclage IPv4	60789	Bouclage IPv4	60790
svchost.exe (UnistackSvcGroup)	8744	192.168.2.101	55517	52.179.236.206	443
svchost.exe (UnistackSvcGroup)	8744	192.168.2.101	55037	52.179.236.206	443
OUTLOOK.EXE	9344	192.168.2.101	58560	52.96.88.162	443
OUTLOOK.EXE	9344	192.168.2.101	51061	40.100.162.178	443
OUTLOOK.EXE	9344	192.168.2.101	50755	52.96.88.130	443
CcmExec.exe	11504	192.168.2.101	58550	192.168.99.111	80
Teams.exe	13788	192.168.2.101	58476	52.113.206.43	443
Teams.exe	13788	192.168.2.101	64640	52.114.128.81	443
Teams.exe	13788	192.168.2.101	63425	52.113.194.132	443
OneDrive.exe	14456	192.168.2.101	53892	52.177.166.224	443

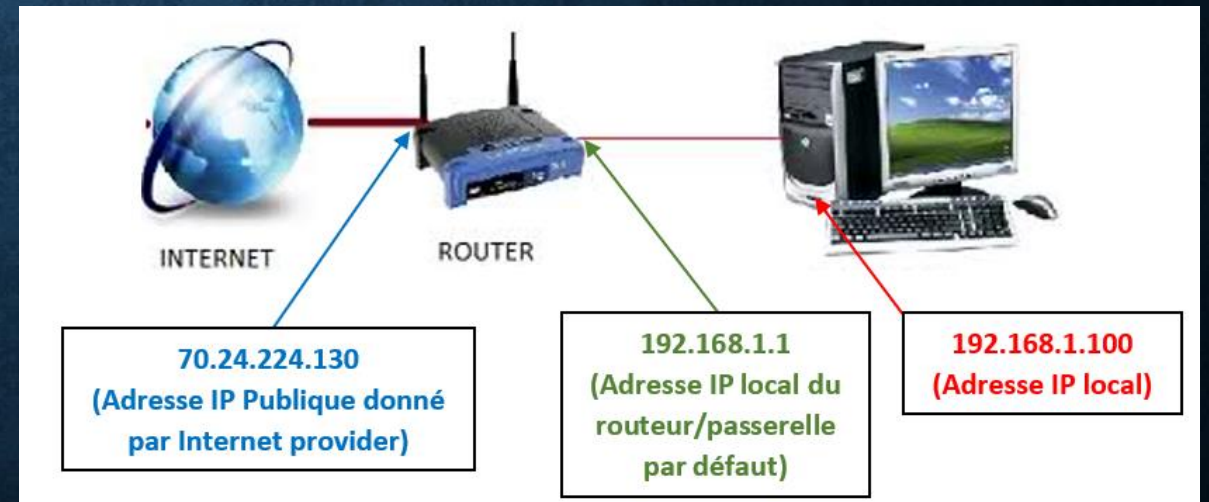
LES PORTS RÉSEAUX - **SCAN DES PORTS**

- Puisque le service est en court de fonctionnement et en attente de connexion, ce dernier peut permettre **une intrusion**.
- Si le service compte **une vulnérabilité**, un pirate peut exploiter celle-ci pour exécuter un logiciel malveillant ou s'introduire dans le système.
- Une technique d'attaque et de découverte consiste **à vérifier tous les ports ouverts d'une machine** pour énumérer les applications et services en cours de fonctionnement.
- On appelle cela le **scan de ports** ou **balayage de ports**.

LES PORTS RÉSEAUX - SCAN DEPUIS INTERNET

- Il existe des services en ligne qui permettent de scanner les ports ouverts. Example: <https://hidemy.name/en/port-scanner/>
- C'est **les ports ouverts de votre routeur** qui seront scanner depuis internet et non votre ordinateur, qui n'est pas directement accessible puisqu'il est placé derrière votre routeur.
- La plupart du temps, les ports vont être affichés comme **filtré** car le pare-feu de votre routeur est activé.

Enter your IP address or domain	Test result						
<input type="text" value="70.24.224.130"/>	<div>Not shown: 998 filtered ports, 1 closed port</div> <table border="1"><thead><tr><th>PORT</th><th>STATE</th><th>SERVICE</th></tr></thead><tbody><tr><td>50001/tcp</td><td>open</td><td>unknown</td></tr></tbody></table> <div>Nmap done: 1 IP address (1 host up) scanned in 20.57 seconds</div>	PORT	STATE	SERVICE	50001/tcp	open	unknown
PORT		STATE	SERVICE				
50001/tcp		open	unknown				
<small>Insert my IP address</small>							
<input type="text" value="Popular ports"/>							
<input type="button" value="Start scanning"/>	<small>If the result is "Host seems down", then the network screen or router of the IP address being checked blocks pings.</small>						



2- PARE-FEU - DÉFINITION

- Un firewall ou pare-feu est **un logiciel** ou **équipement réseau** placé entre deux réseaux pour filtrer les connexions entrantes et sortantes.
- Le pare-feu **autorise** ou **refuse** les connexions légitimes des connexions non légitimes.
- Ces autorisations d'accès peuvent se faire **à partir de règles établies par l'administrateur** ou de **manière automatique** selon par exemple le contenu des paquets réseaux qui transitent.
- Avec un firewall, vous pouvez potentiellement **bloquer le trafic malveillant** provenant d'une attaque ou le trafic sortant provenant d'un malware.

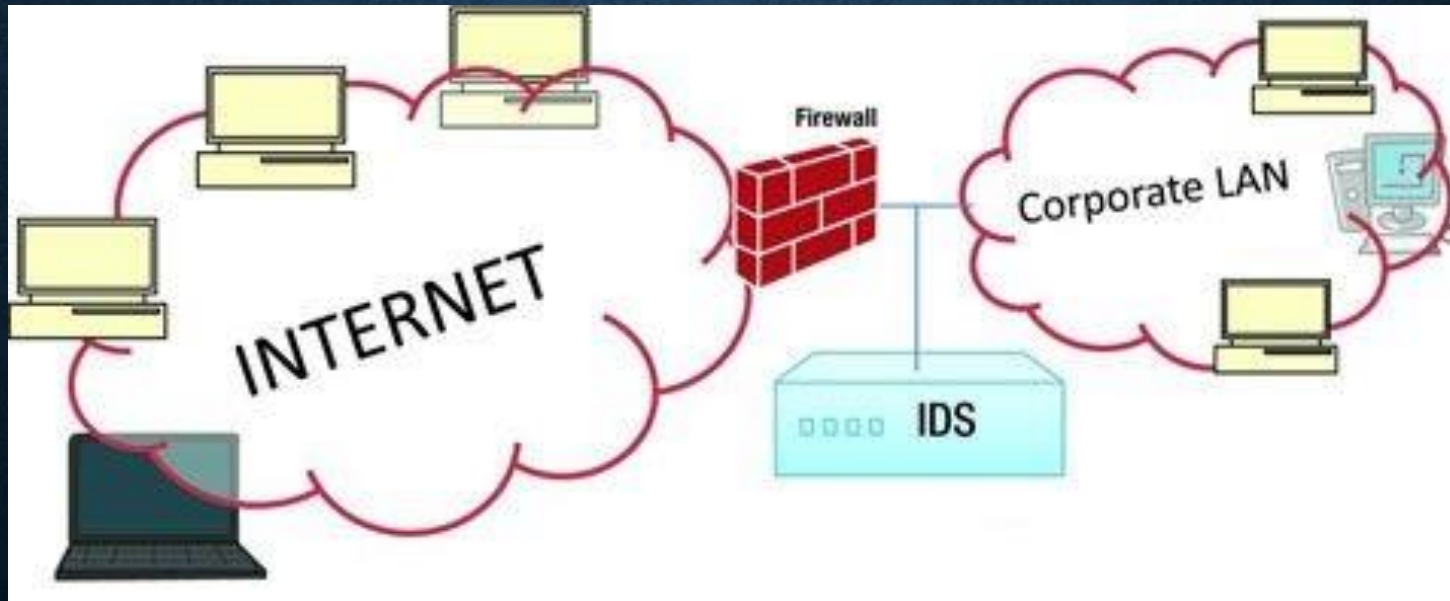


PARE-FEU - GÉNÉRATIONS

- Les premières générations filtre le contenu que sur **les ports de connexion**.
- Ainsi, si vous possédez un site WEB qui tourne sur le **port 80 (HTTP)**, vous devez autoriser les accès sur ce port.
- Toutefois si un malware écoute sur ce port, la connexion sera autorisée.
- Les générations actuelles de pare-feu peut **comprendre et lire les protocoles applicatifs**.
- Ainsi, un pare-feu sait si un paquet concerne une application FTP ou HTTP, en créant les règles appropriées.

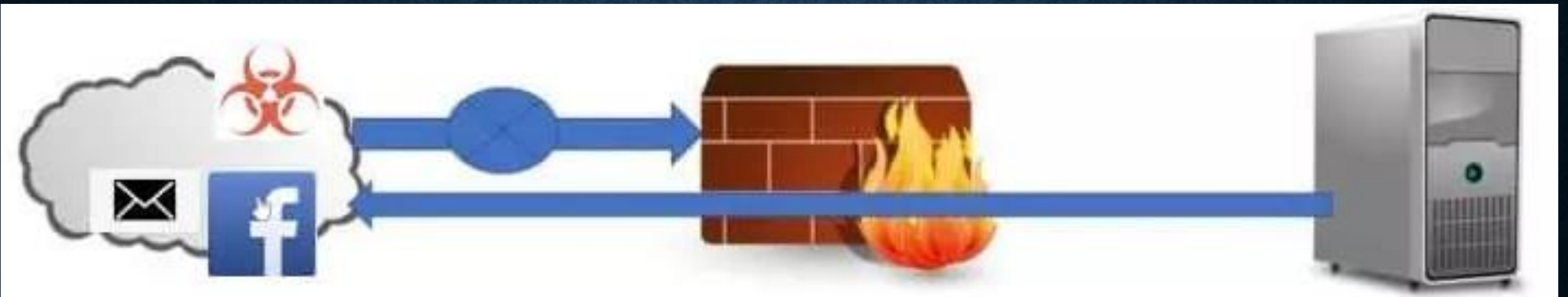
PARE-FEU - GÉNÉRATIONS

- Enfin les **boitiers firewall** embarquent des antivirus, ainsi que des IDS (**Intrusion Detection System** pour système de détection d'intrusion) capable d'analyser les paquets.
- Des **signatures** peuvent être intégrées afin de bloquer des paquets selon leurs contenues afin de bloquer certaines attaques.



3- LE FONCTIONNEMENT DU PARE-FEU

- Le pare-feu fonctionne sur **des règles** qui seront appliquées sur **les paquets entrantes ou sortantes** d'une interface réseaux contrôlées par le pare-feu.
- Celle-ci comporte généralement les données suivantes :
 - Une source (adresse IP ou Hôte) et un port TCP source.
 - Une destination (adresse IP ou Hôte) et un port TCP destination.
 - Parfois on trouve le statut de la connexion (nouvelle, établie).



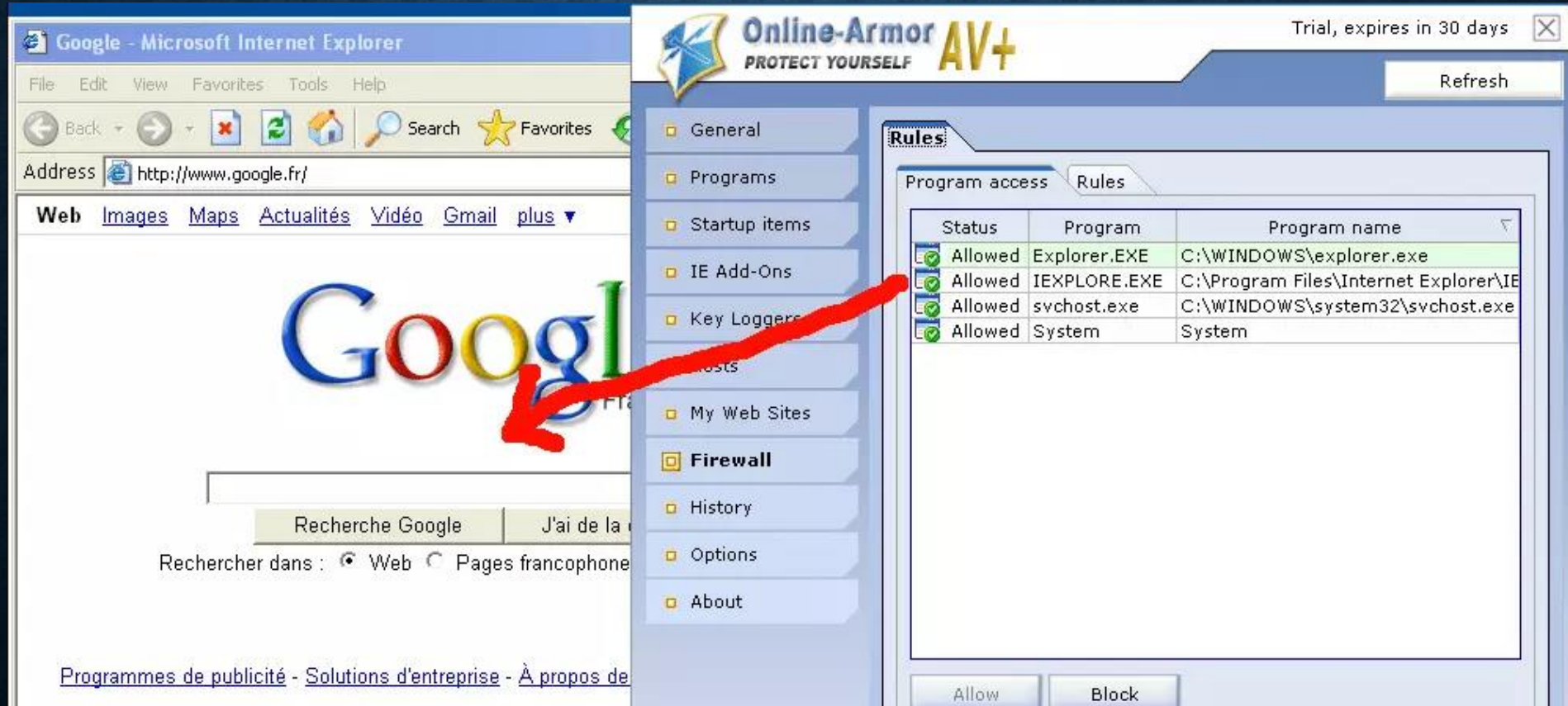
LE FONCTIONNEMENT DU PARE-FEU

- Par exemple, vous pouvez autoriser des connexion provenant de certaines adresses IP en source vers un port particulier puis faire une règle qui interdit toutes les connexions sur ce port.

6	Autoriser	TCP	192.88.134.0/23	443	Activé	
7	Autoriser	TCP	185.93.228.0/22	443	Activé	
8	Autoriser	TCP	66.248.200.0/22	443	Activé	
9	Refuser	TCP	tous	443	Activé	
10	Refuser	TCP	tous	80	Activé	

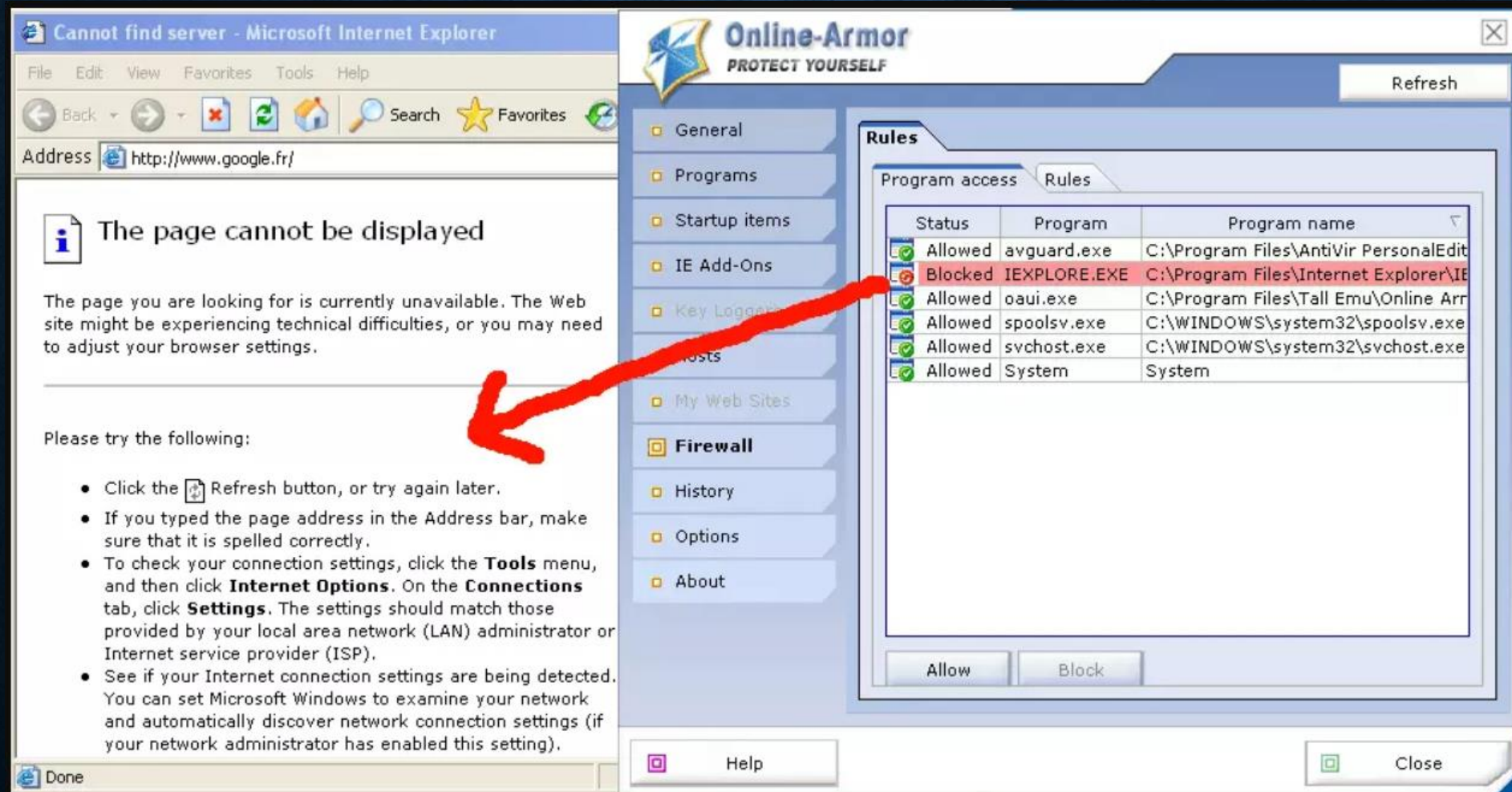
LE FONCTIONNEMENT DU PARE-FEU

- Le pare-feu fonctionne aussi sur **des règles qui autorisent ou interdisent à telles ou telles applications** de se connecter.
- Par exemple, ci-dessous, on constate à droite que le pare-feu autorise le processus iexplore.exe. La connexion vers le site Google est alors possible.



LE FONCTIONNEMENT DU PARE-FEU

- On passe alors Internet Explorer en rouge, interdiction... La connexion sur Google renvoi une erreur.



LE FONCTIONNEMENT DU PARE-FEU

- Lorsqu'un programme voudra établir une connexion entrante ou sortante, le pare-feu stoppera immédiatement la connexion et **vous demandera l'action à effectuer.**
- Vous avez généralement le choix entre :
 - Autoriser une fois la connexion ;
 - Autoriser tout le temps la connexion ;
 - Bloquer une fois la connexion ;
 - Bloquer tout le temps la connexion.
- Comprenez donc que **ces règles sont très importantes**, si vous autorisez un logiciel malveillant, ce dernier pourra se connecter et la connexion vers le centre de contrôle sera effective.
- Un pare-feu bloque automatiquement toute connexion non autorisée.

LE FONCTIONNEMENT DU PARE-FEU

- Les pare-feu sont donc extrêmement utiles pour **prévenir l'installation de logiciels malveillants ou bloquer le fonctionnement des virus.**
- Le Firewall peut entrer en jeu lorsqu'un Trojan Downloader, c'est à dire un trojan (le cheval de troie) qui tente de télécharger du contenu malveillant depuis internet.
- En bloquant le Trojan Downloader, ce dernier ne pourra pas télécharger le trojan et l'installer sur l'ordinateur.
- Le pare-feu peut aussi être utile pour **bloquer la communication entre le cheval de troie et le serveur de contrôle du Hacker.**
- Si le trojan ne peut se connecter il ne pourra pas échanger d'informations et ainsi livrer les données volées.

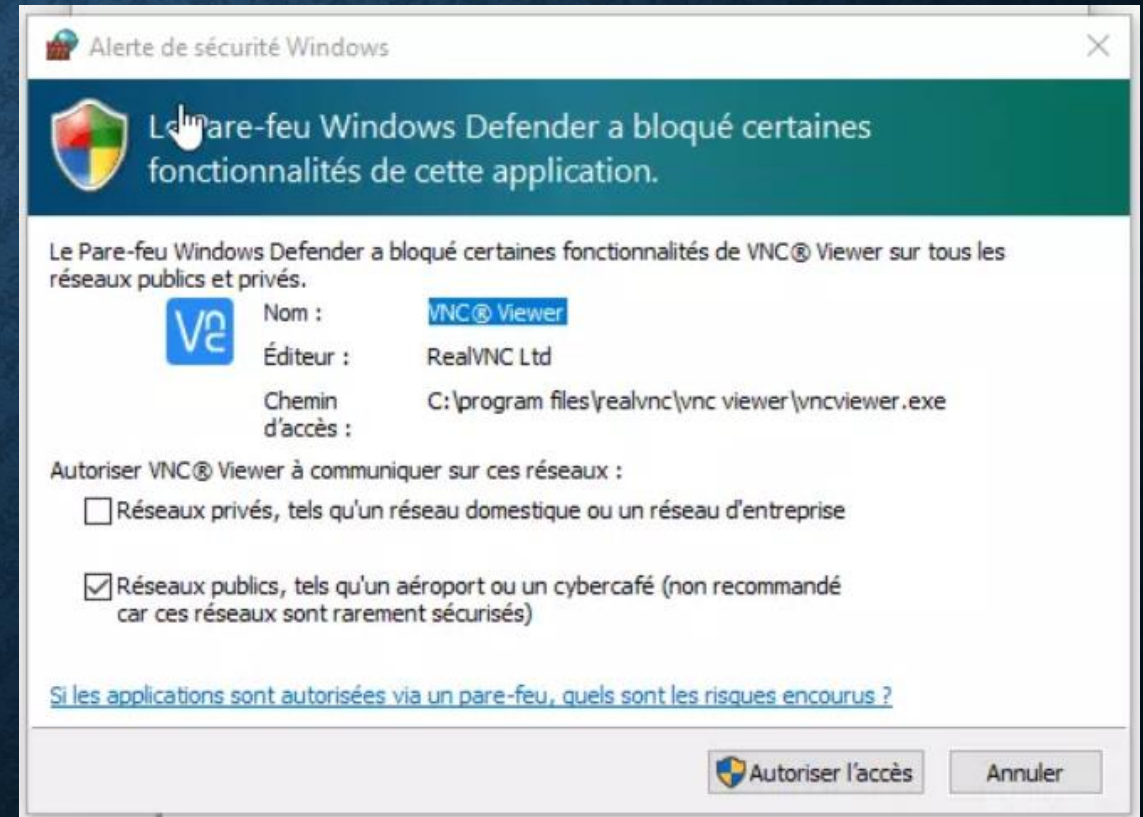
4- AUTRES FONCTIONNALITÉS

- Les fonctionnalités du pare-feu sont généralement différents selon le type de pare-feu (matériel, logiciel pare-feu Windows, etc).
- On trouve aussi un tableau de bord avec **des statistiques de connexions et les journaux** qui permettent de connaître les connexions bloquées ou autorisées par le firewall.

```
[33913009.322422] [IPTABLES DROP] : IN= OUT=eth0 SRC=10.0.0.1 DST=37.187.231.251 LEN=205 TOS=0x00 PREC=0x00 TTL=64 ID=56216 DF PROTO=UDP SPT=43340 DPT=6114 LEN=185
[33913009.351061] [IPTABLES DROP] : IN= OUT=eth0 SRC=10.0.0.1 DST=37.187.231.251 LEN=205 TOS=0x00 PREC=0x00 TTL=64 ID=56220 DF PROTO=UDP SPT=44639 DPT=6151 LEN=185
[33913009.387051] [IPTABLES DROP] : IN= OUT=eth0 SRC=10.0.0.1 DST=37.187.231.251 LEN=186 TOS=0x00 PREC=0x00 TTL=64 ID=56227 DF PROTO=UDP SPT=44470 DPT=6148 LEN=166
[33913009.387764] [IPTABLES DROP] : IN= OUT=eth0 SRC=10.0.0.1 DST=37.187.231.251 LEN=199 TOS=0x00 PREC=0x00 TTL=64 ID=56228 DF PROTO=UDP SPT=50455 DPT=6155 LEN=179
[33913009.388638] [IPTABLES DROP] : IN= OUT=eth0 SRC=10.0.0.1 DST=37.187.231.251 LEN=201 TOS=0x00 PREC=0x00 TTL=64 ID=56229 DF PROTO=UDP SPT=49635 DPT=6125 LEN=181
[33913049.390644] [IPTABLES DROP] : IN= OUT=eth0 SRC=10.0.0.1 DST=107.254.215.205 LEN=676 TOS=0x00 PREC=0x00 TTL=64 ID=21778 DF PROTO=TCP SPT=22 DPT=40828 WINDOW=22
[33913059.165581] [IPTABLES DROP] : IN=eth0 OUT= MAC=00:22:4d:ad:a9:63:10:bd:18:e5:ff:80:08:00 SRC=185.254.322.11 DST=87.187.231.251 LEN=40 TOS=0x00 PREC=0x00 TTL=245 ID=
NDOW=1024 RES=0x00 SYN URGP=0
[33913068.690532] [IPTABLES DROP] : IN= OUT=eth0 SRC=10.0.0.1 DST=37.187.231.251 LEN=205 TOS=0x00 PREC=0x00 TTL=64 ID=3690 DF PROTO=UDP SPT=41525 DPT=6144 LEN=185
[33913068.735789] [IPTABLES DROP] : IN= OUT=eth0 SRC=10.0.0.1 DST=37.187.231.251 LEN=205 TOS=0x00 PREC=0x00 TTL=64 ID=3691 DF PROTO=UDP SPT=41914 DPT=6169 LEN=185
[33913068.778440] [IPTABLES DROP] : IN= OUT=eth0 SRC=10.0.0.1 DST=37.187.231.251 LEN=203 TOS=0x00 PREC=0x00 TTL=64 ID=3700 DF PROTO=UDP SPT=34635 DPT=6174 LEN=183
[33913068.779029] [IPTABLES DROP] : IN= OUT=eth0 SRC=10.0.0.1 DST=37.187.231.251 LEN=199 TOS=0x00 PREC=0x00 TTL=64 ID=3701 DF PROTO=UDP SPT=44648 DPT=6165 LEN=179
[33913068.779739] [IPTABLES DROP] : IN= OUT=eth0 SRC=10.0.0.1 DST=37.187.231.251 LEN=201 TOS=0x00 PREC=0x00 TTL=64 ID=3702 DF PROTO=UDP SPT=40903 DPT=6185 LEN=181
```


5- EXEMPLES DE PARE-FEU – WINDOWS DEFENDER

- Windows 10 intègre un pare-feu, **Windows Defender**, qui est capable de filtrer les connexions entrantes et sortantes pour les applications en cours d'exécution.
- On peut aussi établir ses propres règles selon les protocoles, ports ou adresses IP.
- Lorsqu'une nouvelle application tente d'émettre une connexion, une alerte de sécurité s'affiche et l'utilisateur doit autoriser ou non.
- À partir de là, une règle se crée afin d'autoriser ou non de manière permanente.

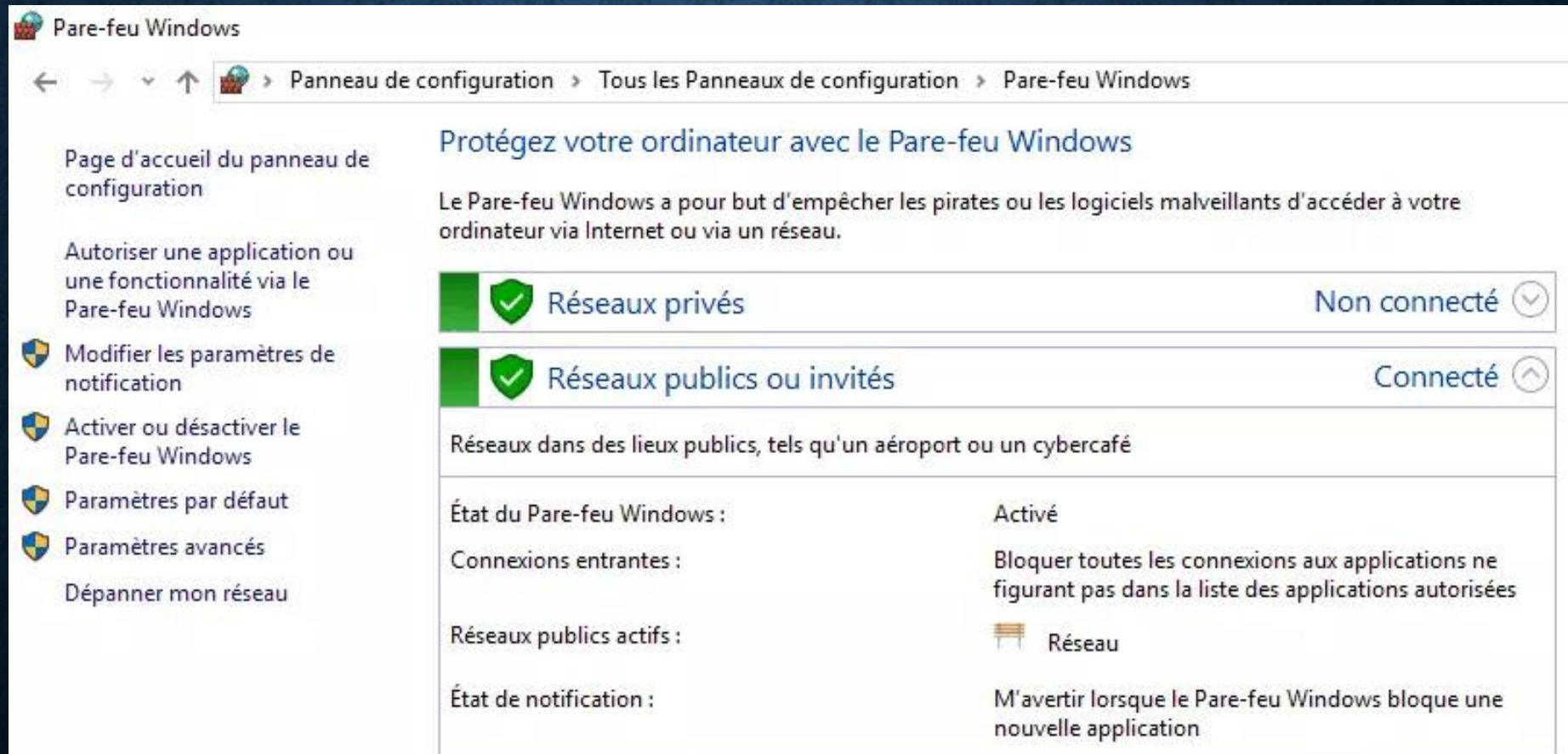


EXEMPLES DE PARE-FEU - WINDOWS DEFENDER

Le pare-feu de Windows se présente sous deux formes :

1. Une **forme simplifiée avec des règles par applications ou ports**.

Les paramètres sont accessibles depuis le **Panneau de configuration de Windows > Pare-feu Windows**.



EXEMPLES DE PARE-FEU - WINDOWS DEFENDER

Applications autorisées

← → ↕ ↑ > Panneau de configuration > Tous les Panneaux de configuration > Pare-feu Windows > Applications autorisées

Autoriser les applications à communiquer à travers le Pare-feu Windows

Pour ajouter, modifier ou supprimer des applications et des ports autorisés, cliquez sur Modifier les paramètres.

Quels sont les risques si une application est autorisée à communiquer ? [Modifier les paramètres](#)

Applications et fonctionnalités autorisées :

Nom	Privé	Public
<input checked="" type="checkbox"/> 3D Builder	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Affichage sans fil	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Analyse de l'ordinateur virtuel	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Arrêt à distance	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Assistance à distance	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Candy Crush Soda Saga	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Cartes Windows	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Compte professionnel ou scolaire	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Conseils Microsoft	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Contacter le Support	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Contacts Microsoft	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Coordinateur de transactions distribuées	<input type="checkbox"/>	<input type="checkbox"/>

Détails... Supprimer

Autoriser une autre application...

EXEMPLES DE PARE-FEU - WINDOWS DEFENDER

2. Une interface plus complexe et avancée où vous pouvez ajouter des règles.

Pare-feu Windows Defender avec fonctions avancées de sécurité

Fichier Action Affichage ?

Pare-feu Windows Defender avec fonctions avan...

Règles de trafic entrant

Règles de trafic sortant

Règles de sécurité de connexion

Analyse

Nom	Groupe	Profil	Activée	Action	Remplacer	Programme	Adresse locale	Adresse distante	Protocole	Port local	Port distant	Utilis...
Avira.SoftwareUpdater.ToastNotifications...		Public	Oui	Bloquer	Non	C:\Program ...	Tout	Tout	TCP	Tout	Tout	Tout
Avira.SoftwareUpdater.ToastNotifications...		Doma	Oui	Autoriser	Non	C:\Program ...	Tout	Tout	TCP	Tout	Tout	Tout
FiddlerProxy		Tout	Oui	Autoriser	Non	C:\Users\ma...	Tout	Tout	TCP	Tout	Tout	Tout
FileZilla Server		Privé ...	Oui	Autoriser	Non	C:\Program ...	Tout	Tout	UDP	Tout	Tout	Tout
FileZilla Server		Doma	Non	Autoriser	Non	C:\Program ...	Tout	Tout	TCP	Tout	Tout	Tout
FileZilla Server		Doma	Non	Autoriser	Non	C:\Program ...	Tout	Tout	UDP	Tout	Tout	Tout
FileZilla Server		Privé ...	Oui	Autoriser	Non	C:\Program ...	Tout	Tout	TCP	Tout	Tout	Tout
Firefox		Public	Oui	Autoriser	Non	C:\program ...	Tout	Tout	TCP	Tout	Tout	Tout
Firefox		Public	Oui	Autoriser	Non	C:\program ...	Tout	Tout	UDP	Tout	Tout	Tout
Firefox (C:\Program Files (x86)\Mozilla Fir...		Privé	Oui	Autoriser	Non	C:\Program ...	Tout	Tout	UDP	Tout	Tout	Tout
Firefox (C:\Program Files (x86)\Mozilla Fir...		Privé	Oui	Autoriser	Non	C:\Program ...	Tout	Tout	TCP	Tout	Tout	Tout
Local TBConsoleUI.exe		Public	Oui	Autoriser	Non	C:\Program ...	Tout	Tout	UDP	Tout	Tout	Tout
Local TBConsoleUI.exe		Public	Oui	Autoriser	Non	C:\Program ...	Tout	Tout	TCP	Tout	Tout	Tout
Local TodoBackupService.exe		Public	Oui	Autoriser	Non	C:\Program ...	Tout	Tout	TCP	Tout	Tout	Tout
Local TodoBackupService.exe		Public	Oui	Autoriser	Non	C:\Program ...	Tout	Tout	UDP	Tout	Tout	Tout
TbService.exe		Public	Oui	Autoriser	Non	C:\Program ...	Tout	Tout	UDP	Tout	Tout	Tout
TbService.exe		Public	Oui	Autoriser	Non	C:\Program ...	Tout	Tout	TCP	Tout	Tout	Tout
@(Microsoft.Messaging_3.37.23004.0_x64...	@(Microsoft.Messaging_3.3...	Tout	Oui	Autoriser	Non	Tout	Tout	Tout	Tous	Tout	Tout	Tout
@(Microsoft.OneConnect_4.1805.1291.0_...	@(Microsoft.OneConnect_4...	Doma...	Oui	Autoriser	Non	Tout	Tout	Tout	Tous	Tout	Tout	Tout
@(Microsoft.SkypeApp_12.1815.209.0_x6...	@(Microsoft.SkypeApp_12.1...	Doma...	Oui	Autoriser	Non	Tout	Tout	Tout	Tous	Tout	Tout	Tout
@(Microsoft.ZuneVideo_10.18052.10711...	@(Microsoft.ZuneVideo_10...	Doma...	Oui	Autoriser	Non	Tout	Tout	Tout	Tous	Tout	Tout	Tout
Affichage sans fil (TCP entrant)	Affichage sans fil	Tout	Oui	Autoriser	Non	%systemroo...	Tout	Tout	TCP	Tout	Tout	Tout
Canal arrière d'infrastructure d'affichage ...	Affichage sans fil	Tout	Oui	Autoriser	Non	%systemroo...	Tout	Tout	TCP	7250	Tout	Tout
Analyse de l'ordinateur virtuel (Demande...	Analyse de l'ordinateur virtuel	Tout	Non	Autoriser	Non	Tout	Tout	Tout	ICMPv4	Tout	Tout	Tout
Analyse de l'ordinateur virtuel (Demande...	Analyse de l'ordinateur virtuel	Tout	Non	Autoriser	Non	Tout	Tout	Tout	ICMPv6	Tout	Tout	Tout
Analyse de l'ordinateur virtuel (NB-Session...	Analyse de l'ordinateur virtuel	Tout	Non	Autoriser	Non	Tout	Tout	Tout	TCP	139	Tout	Tout
Analyse de l'ordinateur virtuel (RPC)	Analyse de l'ordinateur virtuel	Tout	Non	Autoriser	Non	%SystemRo...	Tout	Tout	TCP	Ports dyn...	Tout	Tout
Analyse de l'ordinateur virtuel (Trafic entr...	Analyse de l'ordinateur virtuel	Tout	Non	Autoriser	Non	%SystemRo...	Tout	Tout	TCP	135	Tout	Tout
Règle entrante pour l'arrêt à distance (RP...	Arrêt à distance	Tout	Non	Autoriser	Non	%systemroo...	Tout	Tout	TCP	Mappeur ...	Tout	Tout
Règle entrante pour l'arrêt à distance (TC...	Arrêt à distance	Tout	Non	Autoriser	Non	%systemroo...	Tout	Tout	TCP	Ports dyn...	Tout	Tout
Asphalt 8: Airborne	Asphalt 8: Airborne	Doma...	Oui	Autoriser	Non	Tout	Tout	Tout	Tous	Tout	Tout	Tout
Assistance à distance (DCOM-In)	Assistance à distance	Doma	Oui	Autoriser	Non	%SystemRo...	Tout	Tout	TCP	135	Tout	Tout
Assistance à distance (PNRP-Entrant)	Assistance à distance	Doma...	Oui	Autoriser	Non	%systemroo...	Tout	Tout	UDP	3540	Tout	Tout
Assistance à distance (PNRP-Entrant)	Assistance à distance	Public	Non	Autoriser	Non	%systemroo...	Tout	Tout	UDP	3540	Tout	Tout
Assistance à distance (SSDP TCP - en entr...	Assistance à distance	Doma...	Oui	Autoriser	Non	System	Tout	Sous-réseau local	TCP	2869	Tout	Tout

Actions

Règles de trafic entrant

Nouvelle règle...

Filtrer par profil

Filtrer par état

Filtrer par groupe

Affichage

Actualiser

Exporter la liste...

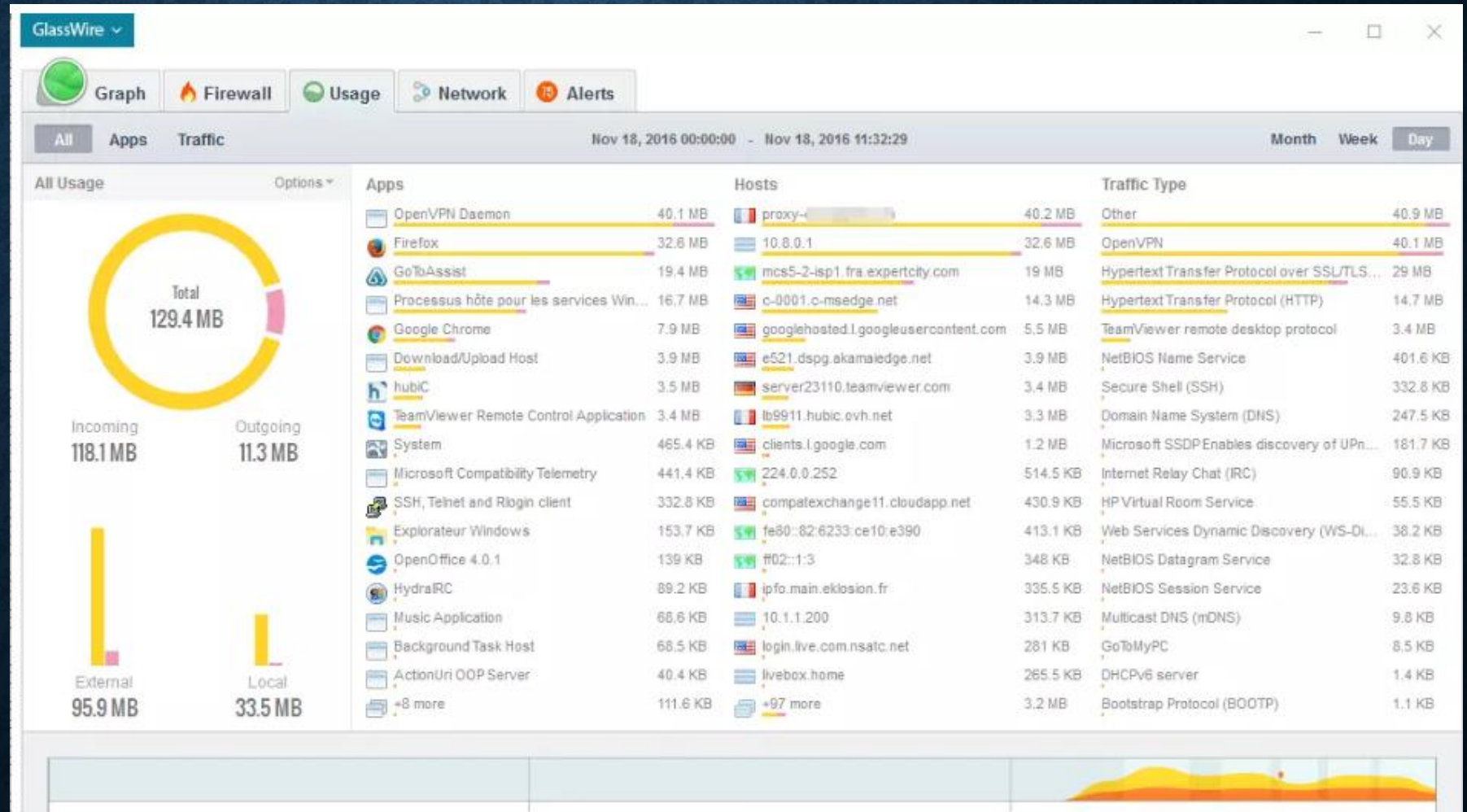
Aide

5. EXEMPLES DE PARE-FEU - PARE-FEU TIERS

- Il existe aussi autres pare-feu pour Windows.
- Globalement le fonctionnement de ces derniers s'avèrent identiques.

- Example:

- Glasswire
- ZoneAlarm
- Comodo Firewall







5. EXEMPLES DE PARE-FEU - ROUTEURS


- Le **routeur à la maison** agit partiellement comme pare-feu pour les ordinateurs du réseau local qui y sont connectés.
- Le routeur n'autorise que les connexions initialisées depuis le réseau local.
- C'est à dire qu'il **va autoriser les connexions sortantes** depuis un ordinateur du réseau local vers internet et bloquer les connexions depuis internet via ces ordinateurs (sauf si un transfert de ports a été configuré).
- Cependant, les connexions sortantes étant autorisées, toute connexion provenant de votre ordinateur vers un site est autorisé, donc **potentiellement le téléchargement d'un Trojan par exemple, sauf si vous installez un pare-feu sur chaque ordinateur.**



EXEMPLES DE PARE-FEU - ROUTEURS

Firewall: Rules: Edit

Edit Firewall rule

Action	<div>Pass ▾</div> <p>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.</p>
Disabled	<div><input type="checkbox"/> Disable this rule</div> <p>Set this option to disable this rule without removing it from the list.</p>
Interface	<div>LAN ▾</div> <p>Choose on which interface packets must come in to match this rule.</p>
TCP/IP Version	<div>IPv4 ▾</div> Select the Internet Protocol version this rule applies to
Protocol	<div>any ▾</div> <p>Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.</p>
Source	<div><input type="checkbox"/> not</div> <p>Use this option to invert the sense of the match.</p> <div>Type: LAN net ▾</div> <div>Address: <input type="text"/> / <input type="text"/> ▾</div>
Destination	<div><input type="checkbox"/> not</div> <p>Use this option to invert the sense of the match.</p> <div>Type: any ▾</div> <div>Address: <input type="text"/> / <input type="text"/> ▾</div>
Log	<div><input type="checkbox"/> Log packets that are handled by this rule</div> <p>Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page)</p>
Description	<div> Default allow LAN to any rule</div> <p>You may enter a description here for your reference.</p>

5. EXEMPLES DE PARE-FEU - **BOITIERS FIREWALL**

- Le **Cisco ASA** est un exemple des **boitiers Firewall** qui existent sous différents modèles et utilisé dans les entreprises.
- Exemple, le pare-feu **Cisco ASA, série 5500-X** est un pare-feu de nouvelle génération conçu pour vous aider à trouver le juste équilibre entre efficacité et productivité.
- Cette solution combine le pare-feu dynamique le plus déployé de l'industrie à un éventail complet de services de sécurité réseau de nouvelle génération, y compris :
 - Robuste **sécurité Web**, sur site ou en nuage;
 - Système **prévention** pour protéger les réseaux contre les menaces connues;
 - Protection complète contre **les menaces et les programmes malveillants**;
 - Pare-feu **ASA** le plus déployé au monde avec **l'accès distant sécurisé**.



EXEMPLES DE PARE-FEU - BOITIERS FIREWALL

- Voici une exemple des règles de **pare-feu Cisco ASA** ainsi que toute la configuration.

The screenshot displays the Cisco ASDM 6.4 for ASA interface, specifically the 'Configuration > Firewall > Access Rules' section. The left sidebar shows the 'Firewall' tree with 'Access Rules' selected. The main pane shows a table of access rules, categorized into 'inside (8 incoming rules)', 'outside (4 incoming rules)', and 'Global (1 implicit rule)'. The table columns include #, Enabled, Source, User, Destination, Service, Action, Hits, Logging, Time, and Description. Below the table, the 'Access Rule Type' is set to 'IPv4 Only'. A diagram at the bottom illustrates the rule configuration: traffic from source IP 188.165.204.75 is permitted to destination IP 82.94.216.250 (abuseat.org) on port 80 (http) via the 'inside' interface.

#	Enabled	Source	User	Destination	Service	Action	Hits	Logging	Time	Description
inside (8 incoming rules)										
1	<input checked="" type="checkbox"/>	188.165.204.75		Akismet	http	Permit	0			
2	<input checked="" type="checkbox"/>	188.165.204.75		Google	http	Permit	88			
3	<input checked="" type="checkbox"/>	188.165.204.75		Twitter	http	Permit	88			
4	<input checked="" type="checkbox"/>	188.165.204.75		stopforumspam	http	Permit	0			
5	<input checked="" type="checkbox"/>	188.165.204.75		abuseat.org	http	Permit	0			
6	<input checked="" type="checkbox"/>	188.165.204.75		any	smtp	Permit	4			
7	<input checked="" type="checkbox"/>	188.165.204.75		any	icmp	Permit	12			
8	<input checked="" type="checkbox"/>	188.165.204.75		any	domain	Permit	5949			
outside (4 incoming rules)										
1	<input checked="" type="checkbox"/>	any		188.165.204.75	http	Permit	5545			
2	<input checked="" type="checkbox"/>	any		188.165.204.75	https	Permit	2001			
3	<input checked="" type="checkbox"/>	any		188.165.204.75	ssh	Permit	3			
4	<input checked="" type="checkbox"/>	any		188.165.204.75	icmp	Permit	6			
Global (1 implicit rule)										
1		any		any	ip	Deny				Implicit rule

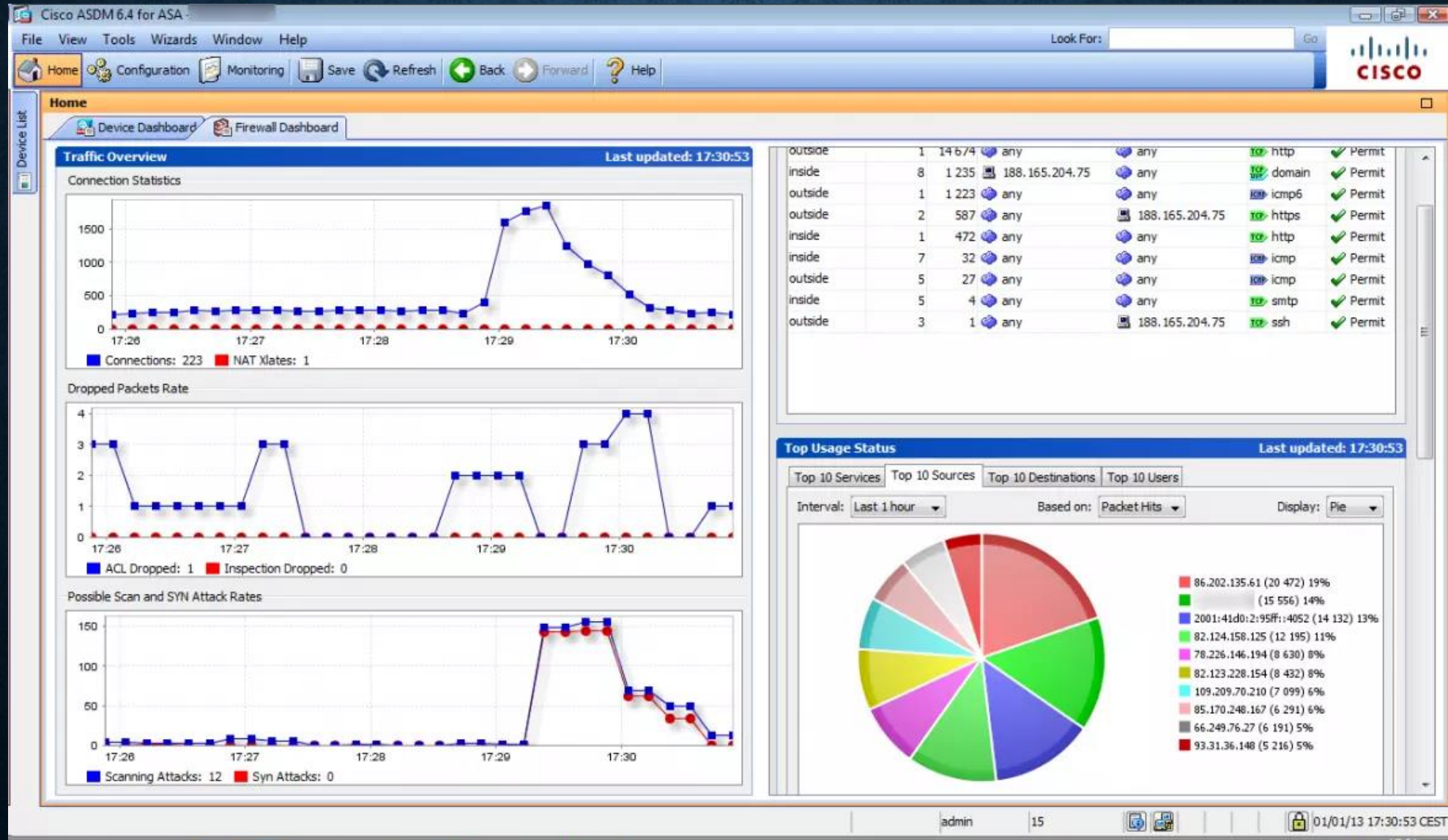
Access Rule Type: ☐ IPv4 and IPv6 ☒ IPv4 Only ☐ IPv6 Only

Diagram: 188.165.204.75 (source) → http → Permit → 82.94.216.250 (abuseat.org) (destination) via inside interface.

Running configuration successfully saved to flash memory. admin 15 01/01/13 19:18:53 CEST

EXEMPLES DE PARE-FEU - BOITIERS FIREWALL

- L'interface du **tableau de bord avec des statistiques** de connexion.



EXEMPLES DE PARE-FEU - BOITIERS FIREWALL

- Enfin **les journaux du pare-feu** avec les paquets dropés en temps réel.

The screenshot shows the Cisco ASDM 6.4 for ASA interface. The 'Latest ASDM Syslog Messages' window is open, displaying a list of firewall logs. The logs are organized into columns: Severity, Date, Time, Syslog ID, Source IP, Source, Destination IP, Destination, and Description. The logs show various events, including scanning, deny inbound UDP, and deny udp src outside/inside.

Severity	Date	Time	Syslog ID	Source IP	Source	Destination IP	Destination	Description
4	Jan 01 2013	11:49:14	733100					[Scanning] drop rate-1 exceeded. Current burst rate is 28 per second, max configured rate is 10; Current average rate is 7 per second, max configured rate is 10
2	Jan 01 2013	11:49:13	106006	fe80::21e:13ff...	2029	ff02::66	2029	Deny inbound UDP from fe80::21e:13ff:fe9:af00/2029 to ff02::66/2029 on interface outside
4	Jan 01 2013	11:49:12	733100					[82.123.228.154] drop rate-1 exceeded. Current burst rate is 28 per second, max configured rate is 10; Current average rate is 5 per second, max configured rate is 10
2	Jan 01 2013	11:49:05	106006	fe80::ee30:91...	2029	ff02::66	2029	Deny inbound UDP from fe80::ee30:91ff:fe0:df80/2029 to ff02::66/2029 on interface outside
4	Jan 01 2013	11:49:04	733100					[Scanning] drop rate-2 exceeded. Current burst rate is 8 per second, max configured rate is 8; Current average rate is 2 per second, max configured rate is 8
2	Jan 01 2013	11:49:04	106006	fe80::21e:13ff...	2029	ff02::66	2029	Deny inbound UDP from fe80::21e:13ff:fe9:af00/2029 to ff02::66/2029 on interface outside
4	Jan 01 2013	11:49:03	106023	87.98.134.198	64867	224.0.0.252	5355	Deny udp src outside:87.98.134.198/64867 dst inside:224.0.0.252/5355 by access-group "outside_access_in" [0x0, 0x0]
2	Jan 01 2013	11:49:03	106006	fe80::194b:ee...	60274	ff02::1:3	5355	Deny inbound UDP from fe80::194b:ee9d:bf6d:7462/60274 to ff02::1:3/5355 on interface outside
4	Jan 01 2013	11:49:03	106023	188.165.204.174	52718	224.0.0.252	5355	Deny udp src outside:188.165.204.174/52718 dst inside:224.0.0.252/5355 by access-group "outside_access_in" [0x0, 0x0]
2	Jan 01 2013	11:49:03	106006	fe80::4123:d6...	53589	ff02::1:3	5355	Deny inbound UDP from fe80::4123:d6ea:ae0b:60e2/53589 to ff02::1:3/5355 on interface outside
4	Jan 01 2013	11:49:03	106023	87.98.134.198	64867	224.0.0.252	5355	Deny udp src outside:87.98.134.198/64867 dst inside:224.0.0.252/5355 by access-group "outside_access_in" [0x0, 0x0]
2	Jan 01 2013	11:49:03	106006	fe80::194b:ee...	60274	ff02::1:3	5355	Deny inbound UDP from fe80::194b:ee9d:bf6d:7462/60274 to ff02::1:3/5355 on interface outside
4	Jan 01 2013	11:49:03	106023	188.165.204.174	52718	224.0.0.252	5355	Deny udp src outside:188.165.204.174/52718 dst inside:224.0.0.252/5355 by access-group "outside_access_in" [0x0, 0x0]
2	Jan 01 2013	11:49:03	106006	fe80::4123:d6...	53589	ff02::1:3	5355	Deny inbound UDP from fe80::4123:d6ea:ae0b:60e2/53589 to ff02::1:3/5355 on interface outside
4	Jan 01 2013	11:48:54	733100					[Scanning] drop rate-1 exceeded. Current burst rate is 24 per second, max configured rate is 10; Current average rate is 6 per second, max configured rate is 10
2	Jan 01 2013	11:48:48	106006	fe80::21e:13ff...	2029	ff02::66	2029	Deny inbound UDP from fe80::21e:13ff:fe9:af00/2029 to ff02::66/2029 on interface outside
4	Jan 01 2013	11:48:48	733100					[82.123.228.154] drop rate-1 exceeded. Current burst rate is 18 per second, max configured rate is 10; Current average rate is 3 per second, max configured rate is 10
2	Jan 01 2013	11:48:39	106006	fe80::21e:13ff...	2029	ff02::66	2029	Deny inbound UDP from fe80::21e:13ff:fe9:af00/2029 to ff02::66/2029 on interface outside
4	Jan 01 2013	11:48:37	106023	188.165.204.75	38406	188.165.204.251	6194	Deny udp src inside:188.165.204.75/38406 dst outside:188.165.204.251/6194 by access-group "inside_access_in" [0x0, 0x0]
4	Jan 01 2013	11:48:37	106023	188.165.204.75	39154	188.165.204.251	6129	Deny udp src inside:188.165.204.75/39154 dst outside:188.165.204.251/6129 by access-group "inside_access_in" [0x0, 0x0]
4	Jan 01 2013	11:48:37	106023	188.165.204.75	54635	188.165.204.251	6135	Deny udp src inside:188.165.204.75/54635 dst outside:188.165.204.251/6135 by access-group "inside_access_in" [0x0, 0x0]
4	Jan 01 2013	11:48:37	106023	188.165.204.75	48567	188.165.204.251	6198	Deny udp src inside:188.165.204.75/48567 dst outside:188.165.204.251/6198 by access-group "inside_access_in" [0x0, 0x0]
4	Jan 01 2013	11:48:37	106023	188.165.204.75	52088	188.165.204.251	6159	Deny udp src inside:188.165.204.75/52088 dst outside:188.165.204.251/6159 by access-group "inside_access_in" [0x0, 0x0]
4	Jan 01 2013	11:48:37	106023	188.165.204.75	37497	188.165.204.251	6164	Deny udp src inside:188.165.204.75/37497 dst outside:188.165.204.251/6164 by access-group "inside_access_in" [0x0, 0x0]
2	Jan 01 2013	11:48:34	106006	fe80::ee30:91...	2029	ff02::66	2029	Deny inbound UDP from fe80::ee30:91ff:fe0:df80/2029 to ff02::66/2029 on interface outside
4	Jan 01 2013	11:48:34	733100					[Scanning] drop rate-1 exceeded. Current burst rate is 2 per second, max configured rate is 10; Current average rate is 5 per second, max configured rate is 10
4	Jan 01 2013	11:48:28	106023	188.165.204.152	138	188.165.204.255	138	Deny udp src outside:188.165.204.152/138 dst inside:188.165.204.255/138 by access-group "outside_access_in" [0x0, 0x0]
4	Jan 01 2013	11:48:28	106023	188.165.204.152	138	188.165.204.255	138	Deny udp src outside:188.165.204.152/138 dst inside:188.165.204.255/138 by access-group "outside_access_in" [0x0, 0x0]
4	Jan 01 2013	11:48:26	106023	188.165.204.100	57789	224.0.0.252	5355	Deny udp src outside:188.165.204.100/57789 dst inside:224.0.0.252/5355 by access-group "outside_access_in" [0x0, 0x0]
2	Jan 01 2013	11:48:26	106006	fe80::e873:4f...	62455	ff02::1:3	5355	Deny inbound UDP from fe80::e873:4f2fd9c4:a483/62455 to ff02::1:3/5355 on interface outside